

AO 106 (Rev. 04/10) Application for Search Warrant

FILED

RECEIVED

NOV 20 2018

## UNITED STATES DISTRICT COURT

for the

Western District of Washington

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
BY DEPUTY

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)Lenovo laptop, Seized from Room 409 at the Mediterranean  
Inn located at 425 Queen Anne Ave N, Seattle, Washington  
98109

Case No.

MJ18-542

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

## Code Section

## Offense Description

18 U.S.C. 371; 22 USC 2778; 18 USC 554; 18 U.S.C. 922(g)(5)(B) Conspiracy; Arms Export Control Act; Smuggling; Alien in Possession of a Firearm

The application is based on these facts:

Please see Affidavit of HSI Special Agent Lindsey Smith

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

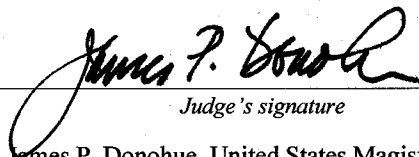
Lindsey Smith, Special Agent (HSI)

Printed name and title

Sworn to before me and signed in my presence.

Date:

20 Nov 2018

City and state: Seattle, Washington


Judge's signature

James P. Donohue, United States Magistrate Judge

Printed name and title

STATE OF WASHINGTON           )  
  )           SS  
COUNTY OF KING             )

## AFFILIANT BACKGROUND

4. As discussed below, there is probable cause to believe that the laptop contains evidence of violations of the Arms Export Control Act, 22 U.S.C. § 2778, and the International Trafficking in Arms Regulations, 22 C.F.R. Part 120 et seq., as well as violations of Title 18, United States Code, Section 554, conspiracy to violate the Arms Export Control Act, 18 U.S.C. § 371, and Alien in Possession of a Firearm, 18 U.S.C. § 922(g)(5)(B).

1       5.     The facts set forth in this Affidavit are based on my own personal  
2 knowledge; information obtained from other individuals during my participation in this  
3 investigation, including other law enforcement officers; interviews of cooperating  
4 witnesses; review of documents and records related to this investigation; communications  
5 with others who have personal knowledge of the events and circumstances described  
6 herein; and information gained through my training and experience.

7       6.     Because this Affidavit is submitted for the limited purpose of establishing  
8 probable cause in support of the application for a search warrant, it does not set forth  
9 each and every fact that I, or others, have learned during the course of this investigation.

10       **RELEVANT LAW PERTAINING TO ARMS EXPORT CONTROL ACT**

11       7.     The Arms Export Control Act ("AECA"), as amended, authorizes the  
12 President of the United States to control the export and import of "defense articles" and  
13 "defense services" by designating those items and services that shall be considered  
14 defense articles and defense services.

15       8.     The President of the United States, by Executive Order 13637, delegated  
16 his statutory authority to promulgate regulations with respect to exports of defense  
17 articles and defense services to the United States Secretary of State. The Department of  
18 State, exercising this authority, promulgated the International Traffic in Arms  
19 Regulations ("ITAR"), 22 C.F.R. Parts 120-130.

20       9.     Items and services constituting "defense articles" and "defense services"  
21 are set forth in the United States Munitions List ("USML"), 22 C.F.R. Part 121.1.  
22 Category I of the USML includes firearms, close assault weapons, and combat shotguns.  
23 As a result, the export of these defense articles requires a license or other written  
24 authorization from the State Department's Directorate of Defense Trade Controls  
25 ("DDTC").

26       10.    The definition of "export" in the ITAR includes the sending or taking of a  
27 defense article out of the United States in any manner. *See* 22 C.F.R. Part 120.17.  
28

11. In the summer of 2016, a confidential informant ("CI") traveled to Lebanon for personal reasons. During his/her travels, the CI visited a firearms store in Tripoli, a city located in northern Lebanon. While at the store, the CI spoke with the shop owner, who identified himself as Hicham DIAB. The CI and DIAB had further conversations at the store on a few other occasions during the CI's trip. Through their discussions, DIAB learned that the CI resided in the United States. DIAB asked the CI if he/she had access to firearms, and, if so, would he/she be willing to sell them to DIAB. DIAB told the CI that he had received M4 barrels from the United States that were smuggled inside of air conditioning tubes.<sup>1</sup> The CI noticed that DIAB had for sale in his shop a variety of firearms, including high-end firearms, Russian-made firearms, and higher-end firearm components from U.S. companies. The CI later returned to the United States and contacted HSI regarding DIAB's interest in obtaining firearms from the United States.<sup>2</sup>

13. During a phone conversation on January 31, 2017, the CI told DIAB he/she had met with the two individuals, *i.e.*, two undercover agents (“UCAs”), and that the UCAs said that the United States is “very rigorous” about exporting firearms and that “without a permit... a permit uh... specifically issued for exporting, [Sighs] they are in

<sup>2</sup> The CI has been paid for his/her efforts in this case.

1 violation of all uh... the federal laws", and that "no doubt they are afraid. These guys are  
2 saying in a very specific way that there is no joke about this matter." DIAB responded,  
3 "You will be working in the 'black market'" and said "there is a lot of gain by going  
4 through the illegitimate way."

5 14. On February 3, 2017, the CI and the UCAs called DIAB. During the call,  
6 the CI introduced the UCAs to DIAB. DIAB said that he wanted 500 Glock, model 19  
7 pistols. DIAB also expressed interest in purchasing 1000 M4 bolt carriers that could  
8 function in fully-automatic M4 rifles. As for payment, DIAB and the UCAs discussed  
9 using a fake company to transfer the funds, as a way to avoid tracing the real source of  
10 the funds. DIAB claimed that he was "1000%" confident that he could successfully  
11 smuggle the guns and parts out of the United States. DIAB and the UCAs agreed to meet  
12 at an upcoming firearms show in Germany.

13 15. On March 21, 2017, UCA1 and the CI met with DIAB in Frankfurt,  
14 Germany. The CI assisted in translating. UCA2 joined part of the meeting via video  
15 conference from the United States. During the meeting, DIAB and the UCAs discussed  
16 procuring firearms and how to ship them. The UCAs told DIAB that the guns needed  
17 "licensing." DIAB stated that the most important thing was for the UCAs to put their  
18 "trust in me and that there is no betrayal." DIAB said: "I do not want the government to  
19 be after me, let it not be any kind of revelations, for example, for later on. This business I  
20 am doing ... the guns and certainly it is not legitimate." UCA1 explained that it was  
21 risky for the UCAs as well, since they would need licenses to complete the export legally.  
22 DIAB stated that "certainly the work we are doing is not legitimate." The CI replied,  
23 "There is danger," to which DIAB responded, "certainly." In regards of how to ship the  
24 items out of the United States, UCA2 said: "If he (DIAB) knows how to do it, we need...  
25 we need to know how to do it because we don't, we don't, [Sighs] we don't, uh... we're  
26 not smugglers man, we're just...we're just gun people... you know?" DIAB replied:  
27 "The weapons will be hidden in something." DIAB asked the UCAs if they had an  
28

1 available space to pack car parts with guns. DIAB told the UCAs: "I am coming to visit  
2 you in the United States, and I'm going teach you a lot of stuff."

3 16. DIAB said wanted only 100, not 500 Glock firearms. DIAB explained that  
4 they needed to build trust before moving onto a bigger deal. UCA2 said that he was  
5 unwilling to do a deal for only 100 guns because of the high risk involved compared to  
6 the low reward of a small deal. DIAB and the UCAs ultimately reached a tentative deal  
7 for 200 Glock firearms.

8 17. Over the span of several months following the meeting, the CI, DIAB, and  
9 the UCAs conducted several phone conversations regarding the firearms deal. The CI  
10 assisted in translating for the UCAs whenever they were present. During one of the  
11 phone conversations on June 26, 2017, DIAB told UCA1 that he would come to the  
12 United States to bring the UCAs money and to show the UCAs how to package the guns.  
13 DIAB said it was very important that he trusted the UCAs to be able to package the guns  
14 correctly. DIAB emphasized that he planned to do a large order in the future and that he  
15 didn't want the UCAs to do a poor job or otherwise his "neck [was] in their hands."  
16 DIAB also asked how much currency he could carry with him to the United States.

17 18. During a phone conversation on August 25, 2017, DIAB told the UCAs that  
18 he had received a visa to travel to the United States. DIAB told the UCAs that it would  
19 be important to ensure that no one would be surveilling them during his visit, and that he  
20 wanted everything to be secure.

21 19. During a phone conversation on September 7, 2017, DIAB told the UCAs  
22 that he wanted to conceal the guns in car parts, such as the front ends of vehicles. DIAB  
23 said he wanted to use Honda parts. DIAB also wanted the UCAs to ensure that the  
24 location of the warehouse where the guns would be packed be secure. DIAB requested  
25 that the UCAs find the warehouse location and the car parts, and that he would travel to  
26 the United States to show the UCAs how he wanted the guns packaged.

27 20. DIAB did not travel to the United State to complete the deal for the 200  
28 guns. However, from October 2017 to August 2018, DIAB and the CI maintained



1 | contact by phone, text, and in person when the CI would travel to Lebanon for personal  
2 | travel. DIAB continually assured the CI that he was trying to solidify the firearms deal  
3 | with his customers.

4 |       21. During a phone conversation on September 20, 2018, DIAB told UCA1  
5 | that he planned to ship a car without a shipping container. He said he would travel to the  
6 | United States to buy a car, package what he could into it, and ship the car in the name of  
7 | another company to Lebanon. DIAB said that this first car shipment would be a test, and  
8 | he requested the UCAs to procure a "bolt carrier with everything that goes with it," and a  
9 | "lower kit" that could fire "single, semi, and burst." UCA1 said that there was too much  
10 | risk and not enough profit in attempting to ship such a small amount, that it would just  
11 | bring trouble. DIAB stated that the "end user" wanted to test the items to make sure the  
12 | items were acceptable, and that if everything was good then very large orders would  
13 | follow. DIAB suggested that he could pack twenty-five to thirty handguns into the car,  
14 | along with the aforementioned parts, and that he would immediately compensate the  
15 | UCAs. UCA1 replied that he and UCA2 would need to decide if they wanted to proceed  
16 | with the deal. DIAB said "time is of the essence" to him and that he wanted the deal to  
17 | be done by November. DIAB said that they should "pray that this first one goes well,  
18 | because what's coming is going to be so good, what the UCAs make in four years, they  
19 | will make in one month."

20 |       22. During a phone conversation on September 26, 2018, UCA1 told DIAB  
21 | that UCA2 wasn't willing to get back into business with DIAB but that he might  
22 | reconsider if the deal looked like it was really going to happen. DIAB said he wanted to  
23 | start business and see how much he could pack into a car. DIAB said he would start  
24 | with an order of 25 handguns and see how they fit in the car. DIAB requested that 30-  
25 | round magazines be included with 10 of the guns. DIAB asked how soon UCA1 could  
26 | be ready. UCA1 replied within 30 days. DIAB then asked UCA1 if they needed money  
27 | in advance. UCA1 said they could get things ready before DIAB got to the United States  
28 | if they were paid in advance. DIAB and the UCA1 agreed on DIAB paying \$10,000 up

1 front to start the order, \$13,000 when DIAB was in the United States, and the remaining  
2 balance of \$11,000 when the shipment was delivered in Lebanon. UCA1 also agreed to  
3 include the bolt carrier that DIAB requested previously. When asked about a vehicle to  
4 use, DIAB requested a 2011 or 2012 Honda CRV, which DIAB agreed to pay for.

5 23. On October 9, 2018, the CI received a text from DIAB showing a receipt of  
6 a wire transfer in the amount of \$10,000 made to UCA1. This wire transfer was  
7 confirmed with the financial institution.

8 24. On October 15, 2018, the CI spoke with DIAB over the phone. During the  
9 call, DIAB told the CI that he was planning to fly to the United States on November 7,  
10 2018, and he would be traveling to the United States with a second individual, a  
11 Canadian citizen, who would help translate and help package the guns into the vehicle.  
12 DIAB also stated he would wire another \$10,000 to the UCAs.

13 25. On October 18, 2018 the CI conducted a recorded phone call with DIAB.  
14 DIAB asked if the UCAs had grenade launchers that attach to M4 rifles, and also asked  
15 about a .50 caliber sniper rifle. The CI replied that grenade launchers are illegal to  
16 possess as civilians, but that the UCAs might have access to them.

17 26. On October 27, 2018, the CI received a text from DIAB with several  
18 photos. The photos included the passport biographical pages for DIAB and a second  
19 individual, Nafez EL MIR, a Canadian citizen who appears to be living in Lebanon.

20 27. On October 28, 2018, the CI spoke with DIAB over the phone. DIAB said  
21 EL MIR would handle the shipping of the car. DIAB also said that he only needed an  
22 hour to pack the car. DIAB inquired about many guns, including custom engraved guns  
23 and sub-machine guns and said he would like to visit a big gun store during his visit in  
24 the United States.

25 28. On October 30, 2018, the CI received a photo from DIAB via text  
26 reflecting a receipt of a wire transfer in the amount of \$10,000 made to UCA1. This wire  
27 transfer was confirmed with the financial institution.



1       29. On November 7, 2018, at approximately 10:40 a.m., Hicham DIAB and  
2 Nafez EL MIR arrived at the Seattle Tacoma International Airport after taking a flight  
3 from Dubai, UAE. They arrived on tourist visas and have no other legal status in the  
4 United States. After passing through passport control and customs clearance, DIAB and  
5 EL MIR were met by the UCAs and the CI.

6       30. EL MIR asked the UCAs if they had a shipping company to handle the  
7 vehicle. EL MIR emphasized that it was important to know whether the car would be  
8 shipped in a container or not.

9       31. The UCAs and CI took DIAB and EL MIR to their hotel to check in.  
10 DIAB then requested that the UCAs take him to their warehouse to see the guns. EL  
11 MIR decided to stay at the hotel to rest.

12       32. The UCAs took the CI and DIAB to the warehouse. At the warehouse,  
13 DIAB was able to inspect the Honda CR-V and weapons that he had purchased from the  
14 UCAs, as well as additional weapons he had requested to see. One of the additional  
15 weapons was a grenade launcher, which DIAB agreed to purchase.

16       33. After inspecting the firearms, the UCAs, the CI, and DIAB went to lunch.  
17 DIAB continued to ask the UCAs for prices for various guns. After lunch, DIAB  
18 requested plastic bubble wrap to pad the firearms for packing in the car. The UCAs, the  
19 CI, and DIAB went to a local hardware store to purchase bubble wrap, tools to  
20 disassemble the car, and plastic wrap. The UCAs, the CI, and DIAB then returned to the  
21 warehouse.

22       34. At the warehouse, DIAB began to disassemble the panels inside the vehicle  
23 and instructed the UCAs to observe him. DIAB then began to wrap the Glock 19  
24 handguns, first in a cloth, then with bubble wrap, and finally in plastic wrap. As DIAB  
25 wrapped the handguns, he started concealing them inside the rear quarter-panel voids of  
26 the car.

27       35. On November 8, 2018, the UCAs and CI met with DIAB and EL MIR for  
28 breakfast. During breakfast, EL MIR initiated conversation regarding how the vehicle

1 would be shipped. EL MIR asked the UCAs if they knew of a company that would ship a  
2 vehicle to Lebanon. EL MIR explained that they had originally planned to buy a car  
3 from a contact in North Carolina, get the car to the UCAs in Seattle to pack, and then  
4 send the car back to the contact in North Carolina to export out of the United States. EL  
5 MIR also mentioned several times that it might be better to transport the car to Florida  
6 and ship the car to Lebanon from there. EL MIR wanted to know under what name they  
7 could ship the vehicle under and suggested the UCAs open a business under which they  
8 could ship cars overseas. EL MIR said he had a company in Lebanon that he uses, and  
9 mentioned that he could open a company in the United States. EL MIR asked if the  
10 UCAs would ship the car in their names. UCA1 said they couldn't put the car in their  
11 names since the guns could come back to the UCAs. EL MIR acknowledged and agreed.  
12 EL MIR suggested he could go to a local Lebanese restaurant and try to befriend a  
13 Lebanese person to put the vehicle in that person's name to ship it. During breakfast,  
14 DIAB began showing UCA1 information on his phone regarding firearm accessories that  
15 he was interested in purchasing.

16 36. Following breakfast, the UCAs, DIAB, and EL MIR traveled to the  
17 warehouse to finish packing the car. At the warehouse DIAB and EL MIR immediately  
18 began disassembling the left rear quarter-panel of the vehicle. DIAB and EL MIR then  
19 filled that void with Glock 19 handguns. They then disassembled the back panel on the  
20 hatchback door and continued concealing Glock 19 handguns, a Smith & Wesson .50  
21 revolver, and one FN Fiveseven pistol inside the voids of the door. DIAB and EL MIR  
22 then began to package all the Glock and FN magazines in the same manner as the  
23 handguns. DIAB placed all the components for a lower kit for a AR15 rifle into one bag,  
24 then wrapped it in plastic. DIAB also wrapped a M203 grenade launcher in the same  
25 manner as the handguns. EL MIR took photos with his cell phone of the vehicle with his  
26 phone.

27 37. DIAB and EL MIR began discussing getting another vehicle as they were  
28 running out of space to conceal all the weapons they were planning to ship. DIAB said

1 they were planning to carry the cleaning kits and additional handgrips included with each  
2 handgun in their luggage on their return trip home.

3 38. Upon exiting the warehouse at approximately 12:30 p.m., HSI and ATF  
4 Special Agents arrested Hicham DIAB and Nafez El MIR. Phones were seized from both  
5 individuals, which are in the process of being searched.

6 39. Surveillance observed that DIAB and EL MIR were staying at the hotel  
7 room that is described in Attachment A-1. On November, 9, 2018, I applied for and  
8 obtained a warrant for the room. Agents found a laptop among the belongings that  
9 appeared to belong to DIAB. I am now seeking a warrant to search this laptop.

10 40. There is probable cause to believe that this laptop contains evidence of the  
11 crime. The fact that DIAB traveled with the laptop strongly suggest that the laptop was  
12 used in the scheme, particularly given that the purpose of his travel was to pick up the  
13 guns to smuggle them to Lebanon. The laptop could have been used in a variety of ways,  
14 including searching for cars to be used in the smuggling operation, contacting the  
15 individual in North Carolina who EL MIR referenced, searching for Lebanese restaurants  
16 in the area, researching guns and gun parts, and otherwise dealing with shipping of the  
17 car.<sup>3</sup>

#### 18 **HOW THE LAPTOP WILL BE SEARCHED**

19 41. Based on my knowledge, training, and experience, I know that laptops can  
20 store information for long periods of time. Similarly, things that have been viewed via  
21 the Internet are typically stored for some period of time on the device used to access the  
22 Internet. This information can sometimes be recovered with forensic tools

23 42. There is probable cause to believe that things that were once stored on the  
24 laptop to be searched may still be stored there, for at least the following reasons:  
25  
26

27 <sup>3</sup> In January 2017, agents provided DIAB with access to an undercover website. Someone using DIAB's credentials  
28 logged onto the site using an iPhone. DIAB did not have an iPhone in his possession. EL MIR did, but it is  
uncertain whether it is the same iPhone that was used to access the site.

1       43. Based on my knowledge, training, and experience, I know that computer  
2 files or remnants of such files can be recovered months or even years after they have been  
3 downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files  
4 downloaded to a storage medium can be stored for years at little or no cost. Even when  
5 files have been deleted, they can be recovered months or years later using forensic tools.  
6 This is so because when a person “deletes” a file on a computer, the data contained in the  
7 file does not actually disappear; rather, that data remains on the storage medium until it is  
8 overwritten by new data.

9       44. Therefore, deleted files, or remnants of deleted files, may reside in free  
10 space or slack space—that is, in space on the storage medium that is not currently being  
11 used by an active file—for long periods of time before they are overwritten. In addition,  
12 a computer’s operating system may also keep a record of deleted data in a “swap” or  
13 “recovery” file.

14       45. Wholly apart from user-generated files, computer storage media—in  
15 particular, computers’ internal hard drives—contain electronic evidence of how a  
16 computer has been used, what it has been used for, and who has used it. To give a few  
17 examples, this forensic evidence can take the form of operating system configurations,  
18 artifacts from operating system or application operation, file system data structures, and  
19 virtual memory “swap” or paging files. Computer users typically do not erase or delete  
20 this evidence, because special software is typically required for that task. However, it is  
21 technically possible to delete this information.

22       46. Similarly, files that have been viewed via the Internet are sometimes  
23 automatically downloaded into a temporary Internet directory or “cache.”

24       47. Forensic evidence. As further described in Attachment B, this application  
25 seeks permission to locate not only electronically stored information that might serve as  
26 direct evidence of the crimes described on the warrant, but also forensic evidence that  
27 establishes how the laptop to be searched was used, the purpose of its use, who used it,  
28

1 and when. There is probable cause to believe that this forensic electronic evidence might  
2 be on the laptop to be searched because:

3 48. Data on the storage medium can provide evidence of a file that was once on  
4 the storage medium but has since been deleted or edited, or of a deleted portion of a file  
5 (such as a paragraph that has been deleted from a word processing file). Virtual memory  
6 paging systems can leave traces of information on the storage medium that show what  
7 tasks and processes were recently active. Web browsers, e-mail programs, and chat  
8 programs store configuration information on the storage medium that can reveal  
9 information such as online nicknames and passwords. Operating systems can record  
10 additional information, such as the attachment of peripherals, the attachment of USB  
11 flash storage devices or other external storage media, and the times the computer was in  
12 use. Computer file systems can record information about the dates files were created and  
13 the sequence in which they were created.

14 49. As explained herein, information stored within a computer and other  
15 electronic storage media may provide crucial evidence of the “who, what, why, when,  
16 where, and how” of the criminal conduct under investigation, thus enabling the United  
17 States to establish and prove each element or alternatively, to exclude the innocent from  
18 further suspicion. In my training and experience, information stored within a computer  
19 or storage media (e.g., registry information, communications, images and movies,  
20 transactional information, records of session times and durations, internet history, and  
21 anti-virus, spyware, and malware detection programs) can indicate who has used or  
22 controlled the computer or storage media. This “user attribution” evidence is analogous  
23 to the search for “indicia of occupancy” while executing a search warrant at a residence.  
24 The existence or absence of anti-virus, spyware, and malware detection programs may  
25 indicate whether the computer was remotely accessed, thus inculcating or exculpating the  
26 computer owner and/or others with direct physical access to the computer. Further,  
27 computer and storage media activity can indicate how and when the computer or storage  
28 media was accessed or used. For example, as described herein, computers typically

1 contain information that log: computer user account session times and durations,  
2 computer activity associated with user accounts, electronic storage media that connected  
3 with the computer, and the IP addresses through which the computer accessed networks  
4 and the internet. Such information allows investigators to understand the chronological  
5 context of computer or electronic storage media access, use, and events relating to the  
6 crime under investigation. Additionally, some information stored within a computer or  
7 electronic storage media may provide crucial evidence relating to the physical location of  
8 other evidence and the suspect. For example, images stored on a computer may both  
9 show a particular location and have geolocation information incorporated into its file  
10 data. Such file data typically also contains information indicating when the file or image  
11 was created. The existence of such image files, along with external device connection  
12 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
13 camera or cellular phone with an incorporated camera). The geographic and timeline  
14 information described herein may either inculcate or exculpate the computer user. Last,  
15 information stored within a computer may provide relevant insight into the computer  
16 user's state of mind as it relates to the offense under investigation. For example,  
17 information within the computer may indicate the owner's motive and intent to commit a  
18 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt  
19 (e.g., running a "wiping" program to destroy evidence on the computer or password  
20 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

21 50. A person with appropriate familiarity with how an electronic device works  
22 may, after examining this forensic evidence in its proper context, be able to draw  
23 conclusions about how electronic devices were used, the purpose of their use, who used  
24 them, and when.

25 51. The process of identifying the exact electronically stored information on a  
26 storage medium that are necessary to draw an accurate conclusion is a dynamic process.  
27 Electronic evidence is not always data that can be merely reviewed by a review team and  
28 passed along to investigators. Whether data stored on a computer is evidence may



1 depend on other information stored on the computer and the application of knowledge  
2 about how a computer behaves. Therefore, contextual information necessary to  
3 understand other evidence also falls within the scope of the warrant.

4 52. Further, in finding evidence of how a device was used, the purpose of its  
5 use, who used it, and when, sometimes it is necessary to establish that a particular thing is  
6 not present on a storage medium.

7 53. Manner of execution. Because this warrant seeks only permission to  
8 examine a device already in law enforcement's possession, the execution of this warrant  
9 does not involve the physical intrusion onto a premises. Consequently, I submit there is  
10 reasonable cause for the Court to authorize execution of the warrant at any time in the  
11 day or night.

12 54. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal  
13 Rules of Criminal Procedure, the warrant I am applying for will permit imaging or  
14 otherwise copying all data contained on the laptop to be searched, and will specifically  
15 authorize a review of the media or information consistent with the warrant.

16 55. In accordance with the information in this affidavit, law enforcement  
17 personnel will execute the search of the laptop pursuant to this warrant as follows:

18 56. Securing the Data. In order to examine the ESI in a forensically sound  
19 manner, law enforcement personnel with appropriate expertise will attempt to produce a  
20 complete forensic image, if possible and appropriate, of the laptop.


21 57. Law enforcement will only create an image of data physically present on or  
22 within the laptop. Creating an image of the laptop will not result in access to any data  
23 physically located elsewhere. However, to the extent that the laptop has previously  
24 connected to devices at other locations, the laptop may contain data from those other  
25 locations.

26 58. Searching the Forensic Images. Searching the forensic images for the items  
27 described in Attachment B may require a range of data analysis techniques. In some  
28 cases, it is possible for agents and analysts to conduct carefully targeted searches that can

1 locate evidence without requiring a time-consuming manual search through unrelated  
2 materials that may be commingled with criminal evidence. In other cases, however, such  
3 techniques may not yield the evidence described in the warrant, and law enforcement  
4 may need to conduct more extensive searches to locate evidence that falls within the  
5 scope of the warrant. The search techniques that will be used will be only those  
6 methodologies, techniques and protocols as may reasonably be expected to find, identify,  
7 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to  
8 this affidavit.

9 **CONCLUSION**

10 59. Based on the forgoing, I submit that there is probable cause to believe that  
11 the property described in Attachment A contains evidence of the crimes identified above,  
12 and therefore I request authorization to search and seize the items that are described in  
13 Attachment B.

14  
15  
16   
17 LINDSEY SMITH, Affiant  
18 Special Agent, HSI

19 SUBSCRIBED AND SWORN before me this 20<sup>th</sup> day of November, 2018.

20  
21   
22 JAMES P. DONOHUE  
23 United States Magistrate Judge  
24  
25  
26  
27  
28

**ATTACHMENT A**  
**PROPERTY TO BE SEARCHED**

The property to be searched is a Lenovo laptop seized from room 409 at the Mediterranean Inn located at 425 Queen Anne Ave N, Seattle, Washington 98109, currently in the possession of HSI Seattle.

This warrant authorizes the forensic examination of the property described above for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

All evidence, fruits, and instrumentalities related to violations the Arms Export Control Act, 22 U.S.C. § 2778, and the International Trafficking in Arms Regulations, 22 C.F.R. Part 120 et seq., as well as violations of Title 18, United States Code, Section 554, conspiracy to violate the Arms Export Control Act, 18 U.S.C. § 371, and Alien in Possession of a Firearm, 18 U.S.C. § 922(g)(5)(B), that is:

1. Information relating to the export of any firearms or components that are covered by the United States Munitions List.
2. Information relating to U.S. export or customs restrictions, regulations, provisions or laws.
3. Information related to travel to the United States.
4. Information relating to the purchase of any vehicles.
5. Information relating to international shipping.
6. Information relating to any individuals located in North Carolina.
7. Information relating to any Lebanese restaurants located in the Western District of Washington.
8. Any address, contact books, or other information containing address information reflecting those involved in any exports, purchase of firearms, or purchase of vehicles.
9. Evidence of user attribution showing who used or owned the device to be searched at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
10. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.